

REMARKS

The present Preliminary Amendment is intended to place the application in better condition for examination. Favorable consideration and allowance of the application are respectfully requested.

5 New claims 37 - 42 have been added.

 Claim 37 is similar to claim 8 except that the subset S2' in claim 37 has different characterization than the characterization recited in claim 8. The subset S2' in claim 37 is characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables a_1, \dots, a_n and
10 coefficients of components involving multiplication of two or more of the n "oil" variables a_1, \dots, a_n in the k polynomial functions $P'_1(a_1, \dots, a_{n+v}, y_1, \dots, y_k), \dots, P'_k(a_1, \dots, a_{n+v}, y_1, \dots, y_k)$ are zero.

 Support for claim 37 is found in transparency 2 of the presentation of Jacques Patarin entitled "The "oil and vinegar" algorithm for signatures" that
15 was presented at the Dagstuhl Workshop on Cryptography in September 1997 and was incorporated by reference in the present application.

 Transparency 2 of the presentation of Jacques Patarin has been copied into the "Background of the Invention" part of the disclosure to conform to the requirements of MPEP §608.01(p). A declaration by Jacques Patarin
20 stating that the amendatory material copied into the disclosure consists of the same material incorporated by reference in the present application accompanies the present Preliminary Amendment.

 Claims 38 and 39 are similar to claims 9 and 10 respectively except that claims 38 and 39 depend from claim 37 rather than from claim 8 as claims 9
25 and 10. Claims 38 and 39 are supported, inter alia, by the specification from the second full paragraph on page 12 through the first full paragraph on page 13.

 Apparatus claims 40 - 42 correspond to method claims 37 - 39 and are similarly supported by the specification.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is now in better condition for examination. Favorable consideration and allowance of the application are respectfully requested.

Respectfully submitted,

5

JULIAN H. COHEN
c/o LADAS & PARRY
26 WEST 61ST STREET
NEW YORK, NEW YORK 10023
REG. NO.: 20302 (212) 708-1887